

Method and assembly for the transfer of sums of money between transferable memories of an IC-card

Publication number: DE19618471

Publication date: 1998-01-08

Inventor: HARTLEIF SIEGFRIED (DE); NIEHAUS HERBERT (DE)

Applicant: DEUTSCHE TELEKOM AG (DE); IBM (US)

Classification:

- international: G07F7/08; G07F7/10; G07F7/08; G07F7/10; (IPC1-7):
G07F19/00; G06F17/60; G06K19/07; H04L9/32

- european: G07F7/08C2B; G07F7/08C2C; G07F7/08C6;
G07F7/10D8P

Application number: DE19961018471 19960508

Priority number(s): DE19961018471 19960508

Also published as:



EP0806747 (A2)

EP0806747 (A3)

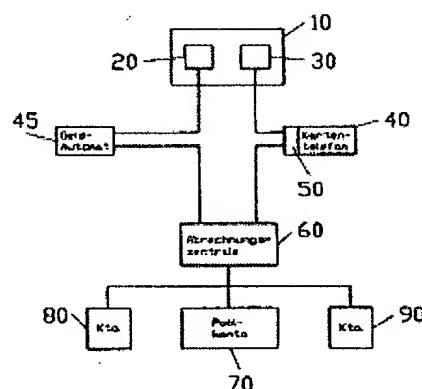
EP0806747 (B1)

Report a data error here

Abstract not available for DE19618471

Abstract of corresponding document: **EP0806747**

The credit transfer method allows a credit amount to be transferred between 2 different memories (20,30) incorporated in the pre-payment card (10) upon insertion of the card in a card reader (40) coupled to a central accounting point (60). The credit amount is transferred from a memory (20) acting as an electronic purse, which is previously loaded with a given credit, after verification of the inserted card via an authentication device (50) associated with the card reader, the credit amount received by a secondary memory (30) with a different purse operator.



Figur

Data supplied from the esp@cenet database - Worldwide



FH

⑬ **BUNDESREPUBLIK
DEUTSCHLAND**



**DEUTSCHES
PATENTAMT**

⑫ **Offenlegungsschrift**
⑩ **DE 196 18 471 A 1**

⑤ Int. Cl.⁸:
G 07 F 19/00
G 06 F 17/60
G 06 K 19/07
H 04 L 9/32

⑳ Aktenzeichen: 196 18 471.1
㉔ Anmeldetag: 8. 5. 96
㉕ Offenlegungstag: 8. 1. 98

DE 196 18 471 A 1

㉑ **Anmelder:**

Deutsche Telekom AG, 53113 Bonn, DE; International
Business Machines Corp., Armonk, N.Y., US

㉒ **Vertreter:**

Kampfenkel, K., Dipl.-Ing., Pat.-Anw., 65193
Wiesbaden

㉓ **Erfinder:**

Hartleif, Siegfried, 64823 Groß-Umstadt, DE;
Niehaus, Herbert, 48165 Münster, DE

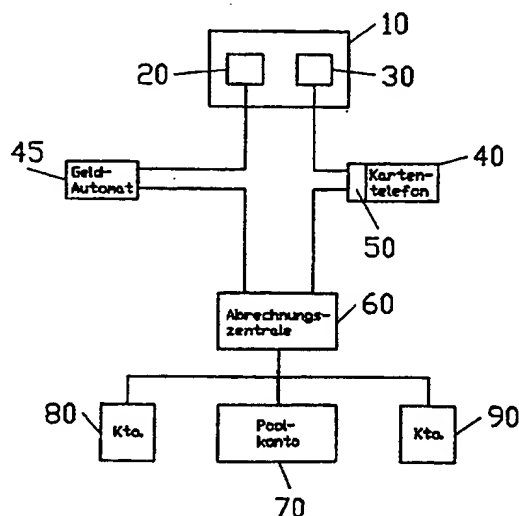
㉔ **Entgegenhaltungen:**

DE 44 37 283 C1
DE 43 33 388 A1
DE 42 43 851 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

㉕ **Verfahren und Anlage zum Transferieren von Geldbeträgen zwischen überschreibbaren Speichern einer Chipkarte**

㉖ Die Erfindung betrifft ein Verfahren sowie eine Anlage zum Transferieren von Geldbeträgen zwischen wenigstens zwei überschreibbaren, verschiedenen Börsenbetreibern zugeordneten Speichern (20, 30) einer Chipkarte (10) mit Hilfe eines einen Kartenleser enthaltenden Endgeräts (40), das mit einer zentralen Einrichtung (60), insbesondere einer Abrechnungszentrale, verbunden werden kann. Der erste, einem ersten Börsenbetreiber zugeordnete Speicher (20) ist mit einem vorbestimmten Geldbetrag geladen. Die Erfindung ermöglicht einem Karteninhaber auf das Guthaben eines Speichers zuzugreifen, wenn der von ihm benötigte Speicher kein Guthaben mehr enthält, ohne den leeren Speicher erneut extern laden zu müssen. Die Erfindung erreicht dies dadurch, daß nach dem Einführen der Chipkarte (10) in den Kartenleser des Endgeräts (40) ein an dem Endgerät eingetragener Geldbetrag aus dem ersten Speicher (20) in den zweiten, einem zweiten Börsenbetreiber zugeordneten Speicher (30) umgeladen wird. Anschließend erzeugt ein dem Endgerät (40) zugeordnetes Sicherheitsmodul (50) einen kryptografisch gesicherten Buchungsdatensatz, der zur weiteren Verrechnung an die zentrale Einrichtung (60) übertragen wird.



DE 196 18 471 A 1

Die Erfindung betrifft ein Verfahren zum Transferieren von Geldbeträgen zwischen wenigstens zwei überschreibbaren Speichern einer Chipkarte mit Hilfe eines Endgerätes, das mit einer zentralen Einrichtung, insbesondere einer Abrechnungszentrale verbunden werden kann gemäß Anspruch 1 sowie eine Anlage zur Durchführung des Verfahrens nach den Ansprüchen 7 und 8.

Seit geraumer Zeit sind Chipkarten, die eine elektronische Geldbörse eines Börsen- oder Diensteanbieters enthalten, erhältlich, mit denen anstelle von Bargeld an dafür vorgesehenen Akzeptanzstellen bezahlt werden kann. Grundsätzlich sind zwei Methoden bekannt, die das Aufladen der elektronischen Geldbörse auf der Chipkarte ermöglichen. Nach der ersten Methode werden die zu ladenden Geldbeträge beispielsweise in bar, mit einer ec-Karte oder einer Kreditkarte vorab bezahlt und anschließend als Geldwerteeinheiten in die elektronische Geldbörse auf der Chipkarte geladen. Nach der anderen Methode wird die Chipkarte in einen Geldautomaten eingeführt und weist sich zunächst gegenüber einem Sicherheitsmodul oder einem Hintergrundsystem aus. Sogleich wird die auf ihr gespeicherte Bankverbindung des Kunden an das Sicherheitsmodul übertragen. Nach der Eingabe des gewünschten Geldbetrages an dem Geldautomaten und dem Laden der elektronischen Börse mit diesem Geldbetrag wird ein Buchungsdatensatz erzeugt, der zum einen das Konto des Karteninhabers mit diesem Geldbetrag belastet und zum anderen diesen Betrag auf dem Konto des Börsenbetreibers gutschreibt. Möchte jedoch ein Kartenherausgeber unterschiedlichen Börsen-Anbietern die Möglichkeit einräumen, die elektronische Geldbörse auf der Chipkarte gemeinsam zu nutzen, führt dies in der Praxis häufig zu Schwierigkeiten. Denn das Betreiben und die Verwaltung eines sogenannten offenen Börsensystems, bei dem mehrere Börsen-Anbieter eine einzige elektronische Geldbörse gemeinsam benutzen, ist ungleich aufwendiger und damit kostenträchtiger als dies bei geschlossenen Börsensystemen, bei denen jedem Börsen-Anbieter eine eigene elektronische Geldbörse auf der Chipkarte zugeordnet ist, der Fall ist. Ein weiterer Nachteil des offenen Börsensystems ist darin zu sehen, daß ein möglicher Mißbrauch der Karte in der Regel kaum zu erkennen ist. Die Schwierigkeiten eines offenen Börsensystems können dadurch vermieden werden, daß der Kartenherausgeber jedem Börsen-Anbieter eine eigene elektronische Geldbörse auf der Chipkarte zuweist, d. h. ein geschlossenes Börsensystem schafft. Dies führt allerdings für den Karteninhaber zu dem Nachteil, daß er auf jeder elektronischen Geldbörse Geld binden muß. Will ein Kunde zum Beispiel eine Geldbörse nutzen, auf der keine Geldwerteeinheiten mehr gespeichert sind, muß er nach einem der oben genannten Methoden erneut Geld investieren, auch wenn auf den übrigen elektronischen Geldbörsen noch ausreichende Guthaben vorhanden sind.

Der Erfindung liegt daher die Aufgabe zugrunde, ein Verfahren und eine Anlage zur Verfügung zu stellen, mit denen die Nachteile der bekannten offenen und geschlossenen Börsensysteme vermieden werden.

Das technische Problem löst die Erfindung mit den Verfahrensschritten des Anspruchs 1 und den Merkmalen der Ansprüche 7 und 8. Vorteilhafte Weiterbildungen sind in den Unteransprüchen genannt.

Die Erfindung beruht auf dem Gedanken, mehrere, auf einer Chipkarte implementierte elektronische Geld-

börsen verschiedener Börsenbetreiber, die ein an sich geschlossenes Börsensystem bilden, koppeln zu können.

Dazu stellt die Erfindung ein Verfahren zum Transferieren von Geldbeträgen zwischen wenigstens zwei überschreibbaren Speichern einer Chipkarte mit Hilfe eines einen Kartenleser enthaltenen Endgeräts bereit, das mit einer zentralen Einrichtung verbunden werden kann, wobei der erste, einem ersten Börsenbetreiber zugeordnete Speicher anfänglich mit einem vorbestimmten Geldbetrag geladen ist. Zunächst wird die Chipkarte in den Kartenleser des Endgeräts eingeführt. Anschließend wird der vorbestimmte Geldbetrag aus dem ersten Speicher in den zweiten, einem zweiten Börsenbetreiber zugeordneten Speicher umgeladen. Nach der Umladeprozedur wird ein Buchungs-Datensatz erzeugt, der zur weiteren Verrechnung an die zentrale Einrichtung übertragen wird. Bevor jedoch Geldbeträge zwischen den Speichern umgeladen werden, führt die Chipkarte mit einem dem Endgerät zugeordneten Sicherheitsmodul oder einem Hintergrundsystem eine gegenseitige, an sich bekannte Authentifizierung durch. Die Chipkarte kann derart programmiert sein, daß sie unter Ansprechen auf ein kryptographisch gesichertes Auslösesignal vom Sicherheitsmodul den am Endgerät eingegebenen Geldbetrag automatisch aus dem ersten Speicher in den zweiten Speicher umlädt. Alternativ fungiert die Chipkarte lediglich als Slave-Einrichtung, die unter Ansprechen auf kryptographisch gesicherte Steuerbefehle vom Sicherheitsmodul den am Endgerät eingegebenen Geldbetrag aus dem ersten Speicher ausliest und in den zweiten Speicher einschreibt. Die zentrale Einrichtung, bei der es sich in der Regel um eine Abbuchungszentrale handelt, sorgt unter Ansprechen auf den Buchungsdatensatz dafür, daß der umgeladene Geldbetrag auf dem Konto des zweiten Börsenbetreibers gutgeschrieben wird und das Konto des ersten Börsenbetreibers mit diesem Betrag belastet wird. Der Buchungsdatensatz kann ebenfalls kryptographisch gesichert werden. Der Börsenbetreiber des ersten Speichers, das ist der sogenannte Hauptbörsen-Betreiber, ist in der Lage, den kryptographisch gesicherten Buchungsdatensatz zu verifizieren. Unter einer kryptographischen Datensicherung versteht man allgemein die Verschlüsselung der zu übertragenden Nutzdaten selbst. Eine kryptographische Datensicherung liegt aber auch dann vor, wenn die Nutzdaten im Klartext übertragen werden, aber zusätzlich ein aus den Nutzdaten gewonnener Nachrichten-Authentifikationscode (MAC von message authentication code) angehängt wird.

Die Erfindung erlaubt einem Kunden auf einfache Art und Weise auf die elektronische Geldbörse eines anderen Börsenbetreibers zugreifen zu können, falls die von ihm benötigte elektronische Geldbörse eines anderen Börsenbetreibers, die auf derselben Chipkarte integriert ist, gerade leer ist.

Mit der Erfindung können die Vorteile eines geschlossenen Börsensystems, insbesondere die Unabhängigkeit der einzelnen Börsenbetreiber und der ihnen auf einer Chipkarte zugewiesenen elektronischen Geldbörsen, bewahrt werden.

Die Erfindung wird nachstehend anhand eines Ausführungsbeispiels in Verbindung mit der beiliegenden Zeichnung näher erläutert.

Die Figur zeigt das prinzipielle Blockschaltbild einer Anlage, mit der das erfindungsgemäße Verfahren zum Transferieren von Geldbeträgen zwischen wenigstens zwei überschreibbaren Speichern einer Chipkarte durchgeführt werden kann. Eine im Verhältnis zu den

übrigen Komponenten stark vergrößert dargestellte Chipkarte 10 enthält einen Speicher 20, der allgemein auch als elektronische Geldbörse bezeichnet wird. Der Speicher 20 sei die Hauptbörse, die einem ersten Börsenbetreiber zugeordnet ist. Bei dem ersten Börsenbetreiber handele es sich beispielsweise um ein Kaufhaus. Auf der Chipkarte 10 ist ein zweiter Speicher 30 implementiert, der als zweite elektronische Geldbörse fungiert und einem anderen Börsenbetreiber zugeordnet ist.

Für die weitere Beschreibung sei angenommen, daß es sich bei dem zweiten Börsenbetreiber um einen Telekommunikations-Netzbetreiber handelt, der unter anderem öffentliche Kartentelefone bereitstellt. Ein derartiges Kartentelefon ist in der Figur mit dem Bezugszeichen 40 versehen. Das Kartentelefon 40 verfügt selbstverständlich über einen Chipkartenleser, der nicht dargestellt ist. Ein Sicherheitsmodul 50, dessen Funktion nachfolgend noch ausführlicher beschrieben wird, ist beispielsweise in dem Kartentelefon 40 integriert; es kann aber auch extern diesem zugeordnet sein. Die Anlage umfaßt ferner an sich bekannte ec-Geldautomaten, an denen der Chipkarteninhaber seine Hauptbörse 20 laden kann. Der Einfachheit halber ist nur der mit 45 bezeichnete ec-Geldautomat dargestellt. Das Kaufhaus besitzt ein Summenkonto 70, auch Poolkonto genannt, über das die gesamten Geldtransaktionen des Karteninhabers mit dem Kaufhaus und dem Telekommunikations-Netzbetreiber abgewickelt werden. Der Karteninhaber verfügt über ein Konto 90, wohingegen der Telekommunikations-Netzbetreiber ein eigenes Konto 80 führt. Jedes Kartentelefon 40 und jeder ec-Geldautomat 45 sind mit einer Abrechnungszentrale 60 verbunden. Die Abrechnungszentrale 60 ist derart ausgebildet, daß sie alle von dem Karteninhaber mit Bezug auf seine Chipkarte 10 gewünschten Geldbewegungen in dem Summenkonto 70, dem Kundenkonto 90 und dem Konto 80 des Telekommunikations-Netzbetreibers abwickeln kann.

Die Funktionsweise der Anlage und das erfindungsgemäße Verfahren werden nunmehr anhand des folgenden Szenarios erläutert. Zunächst sei angenommen, daß der Karteninhaber seine Hauptbörse 20 mit einem Geldbetrag von 50,- DM bereits geladen hat. Dies kann er an dem Geldautomaten 45 oder einem beliebigen elektronischen Cash-Terminal des Kaufhauses vornehmen. Der Geldautomat 45 übermittelt nach der Transaktion des gewünschten Geldbetrages von 50,- DM einen Buchungsdatensatz an die Abrechnungszentrale 60. Die Abrechnungszentrale 60 veranlaßt unter Ansprechen auf den Buchungsdatensatz, daß das Konto 90 des Karteninhabers mit dem Betrag von 50,- DM belastet wird. Gleichzeitig sorgt die Abbuchungszentrale 60 dafür, daß der Geldbetrag auch auf dem Summenkonto 70 des Kaufhauses gutgeschrieben wird. Der Karteninhaber wünscht nunmehr an dem Kartentelefon 40 ein Gespräch zu führen. Überrascht stellt er fest, daß auf der elektronischen Geldbörse 30, die dem Telekommunikations-Netzbetreiber zugeordnet ist, kein Guthaben mehr gespeichert ist. Ohne erneut Geld von seinem Konto 90 abheben zu müssen, kann er dank der Erfindung einen gewünschten Geldbetrag, sagen wir einmal von 20,- DM, von dem Speicher 20 in den Speicher 30 umladen. Dazu führt der Karteninhaber seine Chipkarte 10 in den Kartenleser des Kartentelefons 40 ein. Das Kartentelefon 40 kann beispielsweise die aktuellen Guthaben der Geldbörsen 20 und 30 auf der Chipkarte 10 auslesen und dem Kunden an einem Display anzeigen.

Da auf dem Speicher 30 kein Guthaben mehr gespeichert ist, veranlaßt der Kunde das Umladen des gewünschten Betrages von der Hauptbörse 20 des Kaufhauses auf die Börse 30 des Telekommunikations-Netzbetreibers. Um die Sicherheit beim Geldtransfer zu steigern, wird vor der eigentlichen Geld-Umladeprozedur eine gegenseitige Authentifikation zwischen der eingeführten Chipkarte 10 und dem dem Kartentelefon 40 zugeordneten Sicherheitsmodul 50 durchgeführt. Das Sicherheitsmodul 50 überzeugt sich davon, daß die eingeführte Chipkarte 10 echt ist. Ebenfalls überzeugt sich die Chipkarte 10 davon, daß das Endgerät 40 bzw. das Sicherheitsmodul 50 echt ist. Nach einer positiven Authentifizierung gibt der Karteninhaber den gewünschten Betrag von 20,- DM, der von dem Speicher 20 in den Speicher 30 umgeladen werden soll, an dem Kartentelefon 40 ein. Die Chipkarte 10 wird im Slave-Modus betreiben, d. h. die Umladeprozedur wird von außen, beispielsweise vom Sicherheitsmodul 50 gesteuert. Zunächst wird der Karteninhaber von dem Kartentelefon 40 aufgefordert, seine persönliche Geheimnummer einzugeben. Nach einer Prüfung der Geheimnummer auf Richtigkeit liest das Kartentelefon 40 das Verfallsdatum und die Kartennummer aus der Chipkarte 10 aus und überprüft, ob das Verfallsdatum abgelaufen ist und ob ggf. die Kartennummer in einer Sperrdatei steht. Die Prüfung hat ergeben, daß das Verfallsdatum weder abgelaufen ist noch daß die Kartennummer in einer Sperrdatei steht. Der Karteninhaber leitet an dem Kartentelefon 40 die Umladeprozedur mittels einer Tastenfolge ein, woraufhin das dem Kartentelefon 40 zugeordnete Sicherheitsmodul 50 zunächst einen kryptographisch abgesicherten "Verringerungsbefehl" an die Chipkarte 10 übermittelt. Unter Ansprechen auf den Verringerungsbefehl reduziert die Chipkarte 10 das Guthaben in der Hauptbörse 20, um den im Verringerungsbefehl genannten Geldbetrag von 20,- DM und überträgt eine kryptographisch gesicherte Antwort an das Sicherheitsmodul 50 zurück. Das Sicherheitsmodul 50 überträgt einen kryptographisch gesicherten "Umlade"-Befehl an die Chipkarte 10, die unter Ansprechen auf den Umladebefehl den aus dem Speicher 20 ausgelesenen Betrag von 20,- DM in den Speicher 30 einschreibt und wiederum eine kryptographisch gesicherte Antwort an das Sicherheitsmodul 50 zurückschickt. Nachdem die Umladeprozedur abgeschlossen ist, erzeugt das Sicherheitsmodul 50 einen kryptographisch gesicherten Buchungsdatensatz, der dem umgeladenen Guthaben entspricht. Der kryptographisch gesicherte Buchungsdatensatz wird im nächsten Schritt zu der Abrechnungszentrale 60 übermittelt. Die Abrechnungszentrale 60 veranlaßt nach Empfang des Buchungsdatensatzes, daß das Summenkonto 70 des Kaufhauses mit dem umgeladenen Betrag von 20,- DM belastet wird. Mit anderen Worten verfügt der Speicher 20 nach der Umladeprozedur nur noch über ein Guthaben von 30,- DM. Gleichzeitig sorgt die Abrechnungszentrale 60 dafür, daß der von dem Speicher 20 auf den Speicher 30 umgeladene Geldbetrag von 20,- DM auf dem Konto 80 des Telekommunikations-Netzbetreibers gutgeschrieben wird. Das erfindungsgemäße Verfahren sieht vor, daß der kryptographisch abgesicherte Buchungsdatensatz jederzeit von dem Kaufhaus überprüft werden kann.

Anstatt die Umladeprozedur eines vorbestimmten Geldbetrages von dem Hauptspeicher 20 in den Speicher 30 unter Steuerung des Sicherheitsmodul 50 durchführen zu lassen, kann die Chipkarte 10 derart programmiert sein, daß sie unter Ansprechen auf einen krypto-

graphisch gesicherten Auslösebefehl vom Sicherheitsmodul 50 die Umladeprozedur selbständig ausführt.

Patentansprüche

1. Verfahren zum Transferieren von Geldbeträgen zwischen wenigstens zwei überschreibbaren Speichern (20, 30) einer Chipkarte (10) mit Hilfe eines Kartenleser enthaltenen Endgeräts (40), das mit einer zentralen Einrichtung (60) verbunden werden kann, wobei der erste, einem ersten Börsenbetreiber zugeordnete Speicher (20) mit einem vorbestimmten Geldbetrag geladen ist, mit folgenden Verfahrensschritten:

a) Einführen der Chipkarte (10) in den Kartenleser des Endgeräts (40),

b) Umladen eines vorbestimmten Geldbetrags aus dem ersten Speicher (20) in den zweiten, einem zweiten Börsenbetreiber zugeordneten Speicher (30),

c) Erzeugen eines Buchungs-Datensatzes, der zur weiteren Verrechnung an die zentrale Einrichtung (60) übertragen wird.

2. Verfahren zum Transferieren von Geldbeträgen nach Anspruch 1, gekennzeichnet durch das gegenseitige Authentifizieren der eingeführten Chipkarte (10) mit einem dem Endgerät (40) zugeordneten Sicherheitsmodul (50).

3. Verfahren zum Transferieren von Geldbeträgen nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß das Umladen des vorbestimmten Geldbetrags vom ersten (20) in den zweiten Speicher (30) durch einen kryptographisch gesicherten Befehl eingeleitet und anschließend automatisch in der Chipkarte (10) durchgeführt wird.

4. Verfahren zum Transferieren von Geldbeträgen nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Chipkarte (10) unter Ansprechen auf kryptographisch gesicherte Befehle den vorbestimmten Geldbetrag aus dem ersten Speicher (20) ausliest und anschließend in den zweiten Speicher (30) einschreibt.

5. Verfahren zum Transferieren von Geldbeträgen nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß der in Schritt c) erzeugte Buchungs-Datensatz kryptographisch gesichert und zur zentralen Einrichtung (60) übertragen wird und daß die zentrale Einrichtung (60) mit Hilfe des empfangenen Buchungs-Datensatzes veranlaßt, daß ein Summenkonto (70) des ersten Börsenbetreibers mit dem umgeladenen Geldbetrag belastet und der umgeladene Geldbetrag auf einem Konto (80) des zweiten Börsenbetreibers gutgeschrieben wird.

6. Verfahren zum Transferieren von Geldbeträgen nach Anspruch 5, dadurch gekennzeichnet, daß der kryptographisch gesicherte Buchungs-Datensatz vom ersten Börsenbetreiber verifiziert werden kann.

7. Anlage zur Durchführung des Verfahrens nach einem der Ansprüche 1—6, mit folgenden Merkmalen:

wenigstens eine Chipkarte (10), die einen ersten, einem ersten Börsenbetreiber zugeordneten Speicher (20) und wenigstens einen zweiten, einem zweiten Börsenbetreiber zugeordneten Speicher (30) enthält,

wenigstens ein von einem der Börsenbetreiber betriebenes Endgerät (40) mit einem Kartenleser,

eine zentrale Einrichtung (60), mit der das Endgerät (40) verbunden ist,

ein dem ersten Börsenbetreiber zugeordnetes Summenkonto (70), ein dem zweiten Börsenbetreiber zugeordnetes Konto (80) und ein Kundenkonto (90), auf die die zentrale Einrichtung (60) zugreifen kann, und

ein dem Endgerät (40) zugeordnetes Sicherheitsmodul (50) dadurch gekennzeichnet, daß die Chipkarte (10) derart programmierbar ist, daß sie unter Ansprechen auf ein vom Endgerät (40) oder vom Sicherheitsmodul (50) erzeugtes Auslösesignal automatisch einen vorbestimmten, am Endgerät (40) eingebbaren Geldbetrag aus dem ersten Speicher (20) in den zweiten Speicher (30) umlädt und daß das Sicherheitsmodul (50) einen kryptographisch gesicherten Buchungs-Datensatz erzeugt und zur zentralen Einrichtung (60) zu weiteren Verrechnungen übermittelt.

8. Anlage zur Durchführung des Verfahrens nach einem der Ansprüche 1—6, mit folgenden Merkmalen:

wenigstens eine Chipkarte (10), die einen ersten, einem ersten Börsenbetreiber zugeordneten Speicher (20) und wenigstens einen zweiten, einem zweiten Börsenbetreiber zugeordneten Speicher (30) enthält,

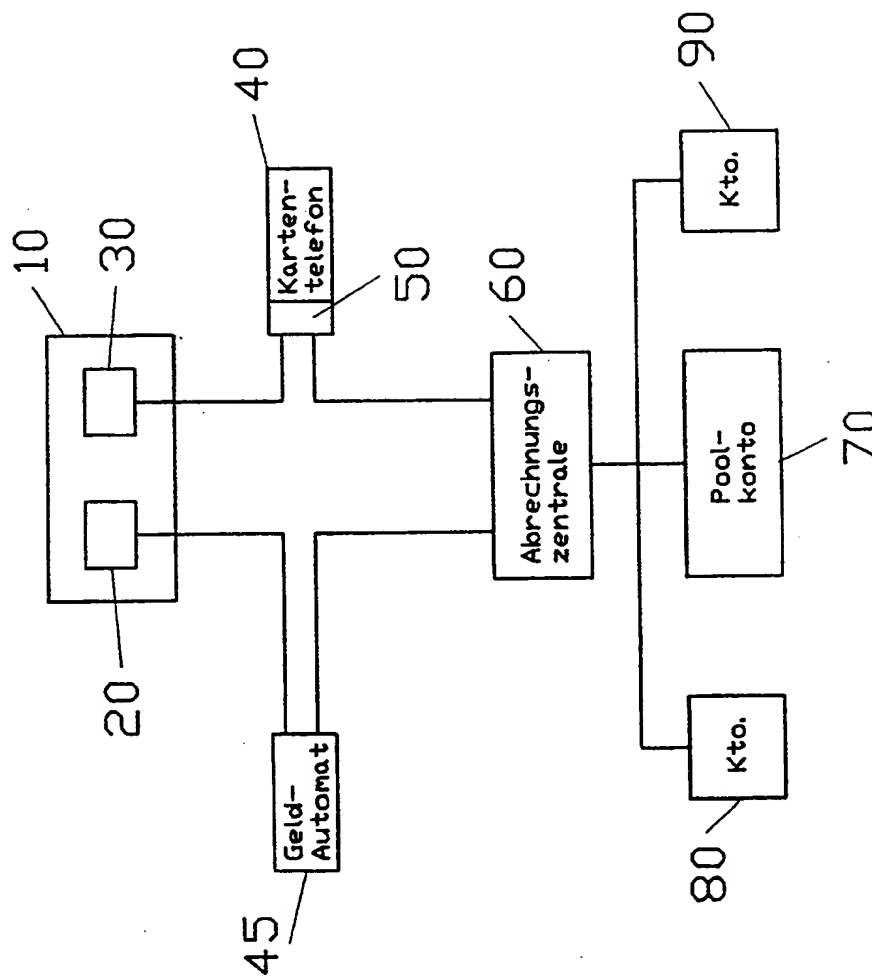
wenigstens ein von einem der Börsenbetreiber betriebenes Endgerät (40) mit einem Kartenleser, eine zentrale Einrichtung (60), mit dem das Endgerät (40) verbunden ist,

ein dem ersten Börsenbetreiber zugeordnetes Summenkonto (70), ein dem zweiten Börsenbetreiber zugeordnetes Konto (80) und ein Kundenkonto (90), auf die die zentrale Einrichtung (60) zugreifen kann, und

ein dem Endgerät (40) zugeordnetes Sicherheitsmodul (50) dadurch gekennzeichnet, daß unter Steuerung des Sicherheitsmoduls (50) die Chipkarte (10) einen vorbestimmten, am Endgerät (40) eingebbaren Geldbetrag aus dem ersten Speicher (20) ausliest und anschließend in den zweiten Speicher (30) umlädt und daß das Sicherheitsmodul (50) einen kryptographisch gesicherten Buchungs-Datensatz erzeugt und zur zentralen Einrichtung (60) zu weiteren Verrechnungen übermittelt.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -



Figur 1